IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:		Atty. Docket No.:	000479.00001
Mark M. Stephenson, et al.			
Serial No.:	09/824,132	Group Art Unit:	2145
Filed:	April 3, 2001	Examiner:	Bhatia, Ajay M.
For:	System and Method for Projecting Content Beyond Firewalls	Confirmation No.:	8931

RESPONSE TO NOTICE OF NON-COMPLIANT APPEAL BRIEF

U.S. Patent and Trademark Office
Customer Service Window
Mail Stop - Appeal
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

This is in response to the Notice of Non-Compliant Appeal Brief mailed on January 18, 2008. As directed by MPEP § 1205.03(B), "When the Office holds the brief to be defective solely due to appellant's failure to provide a summary of the claimed subject matter as required by 37 CFR 41.37(c)(1)(v), an entire new brief need not, and should not, be filed. Rather, a paper providing a summary of the claimed subject matter as required by 37 CFR 41.37(c)(1)(v) will suffice."

Contrary to the allegation in the Notice, the appeal brief as originally filed fully complied with the requirements of 37 CFR 41.37(c)(1)(v). The alleged deficiency was that "Appellant has not provided summary of dependant claims argued separately (claims 56, 59, 60, 63, 70, 72, 80, 78)." The regulation, however, does not require a summary of every dependent claim argued separately. It requires only that, for every dependent claim argued separately, "every means plus function and step plus function as permitted by 35 U.S.C. 112, sixth paragraph, must be identified and the structure, material, or acts described in the specification as corresponding to each claimed function, must be set forth with reference to the specification by page and line number, and to the drawing, if any, by reference characters." No such means plus function or step plus function limitations are recited in any of the identified dependent claims, nor did Applicant ever suggest that these dependent claims contained any such limitations. Hence, the regulation does not require any summary of those dependent claims. Nevertheless, to expedite consideration of this appeal, Appellant hereby re-submits the Summary of Claimed Subject Matter section, including a summary of the dependent claims, none of which recites any means plus function or step plus function limitations.

No fee is believed to be necessary to enter this paper. However, the Commissioner is hereby authorized to charge our Deposit Account No. 19-0733 for any fees necessary to enter or consider this paper.

SUMMARY OF CLAIMED SUBJECT MATTER

37 C.F.R. § 41.37(c)(1)(v)

In making reference herein to various embodiments in the specification text and/or drawings to explain the claimed invention, Appellants do not intend to limit the claims to those embodiments; all references to the specification and drawings are illustrative unless otherwise explicitly stated.

Two computers each protected behind separate firewalls cannot easily exchange data over a network because the firewalls hide the computers from each other. Although HTTP allows bi-directional communication between a computer behind a firewall and an HTTP server on the other side of the firewall, HTTP does not allow generalized communication between two computers each protected by a firewall because HTTP follows a client/server communication paradigm (i.e., one computer must act as the client, the other as the server). Page 1, lines 18-24 to page 2, line 6, paragraph [05]. Requiring that the firewalls be modified to accommodate communication is cumbersome and undesirable, since system administrators must be involved in the process and must make changes to the firewalls, and the resulting changes can compromise security. Page 2, lines 7-18 (paragraph [06]).

According to various embodiments of the invention, an intermediate computer located between the two firewalls is configured to create connections between two endpoint computers, wherein each endpoint initiates a connection with the intermediate computer. In this way, the intermediate computer enables the two computers to communicate bi-directionally as if they are connected together over the same private network without the need to modify either firewall. Page 7, lines 15-22 (paragraph [35]). Four independent claims on appeal recite features of this approach.

Independent Claim 55

Independent claim 55 recites a method of communicating between computers, comprising the steps of:

(1) transmitting from a first computer (FIG. 1, client 101) to an intermediate server computer (FIG. 1, server 107) a first HTTP POST message through a firewall (FIG. 1, firewall 106, page 7 lines 1-14) that is open to outbound Internet traffic (page 6 lines 12-19, paragraph [33]), wherein the first HTTP POST message requests establishment of a connection between the first computer and the intermediate server computer over a first return path (FIG. 5A, step 506, page 7 lines 1-14, paragraph [34], page 22 lines 1-27, paragraphs [106] to [107]);

(2) receiving from the intermediate server computer a response including a connection identifier corresponding to the first return path (FIG. 5A, step 507, page 21, lines 9-12, paragraph [103], page 22 lines 1-27, paragraphs [106] and [107]);

(3) periodically transmitting from the intermediate server computer to the first computer a "keep alive" message over the first return path, if no further messages are sent to the first computer within a period of time (page 13 lines 6-8, paragraph [61], page 23 lines 1-10);

(4) exchanging encryption keys between the first computer and the intermediate server computer (FIG. 5A, step 508, page 13 lines 16-24, paragraph [63], page 24 lines 2-10);

(5) repeating steps (1) through (4) between a second computer (FIG. 1, client 115) and the intermediate server computer (FIG. 1, server 107, through second firewall 113), thereby creating a second return path between the second computer and the intermediate server computer (FIG. 5B, step 512 , page 27 lines 3-7, page 7 lines 1-14, paragraph [34]);

(6) transmitting encrypted information from the first computer through the firewall to the intermediate server computer using further HTTP POST messages (FIG. 5C, step 514; page 3 lines 8-12, paragraph [08], page 8 lines 17-24, paragraph [40]); and

(7) transmitting the encrypted information from the intermediate server over the second return path (FIG. 5C, step 516, page 3 lines 8-12, paragraph [08], page 7 lines 11-14, paragraph [34], page 8 lines 17-24, paragraph [40]).

Independent Claim 57

Independent method claim 57 recites a method of communicating between a first computer (FIG. 1, client 101) protected by a first firewall (FIG. 1, firewall 106) and a second computer (FIG. 1, client 115) protected by a different second firewall (FIG. 1, firewall 113), from the perspective of an intermediate third computer (FIG. 1, server 107), comprising the steps of:

(1) at a third computer (FIG. 1, server 107) situated between the first firewall and the different second firewall, receiving a first HTTP message (FIG. 5A, step 506, page 7 lines 1-14, paragraph [34]) from the first computer through a first firewall that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic (page 6 lines 12-19, paragraph [33], page 7 lines 1-14, paragraph [34]);

(2) from the third computer, sending a first response message to the first computer through the first firewall, thereby establishing a first receive channel through the first firewall (page 22, lines 1-27, paragraphs [106] and [107]), wherein the first response message is linked to the first HTTP message (page 22 lines 19-22, paragraph [107]);

(3) at the third computer, receiving a second HTTP message from the second computer through a different second firewall that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic (FIG. 5B, step 512, page 7 lines 1-14, paragraph [34]);

(4) from the third computer, sending a second response message to the second computer through the second firewall, thereby establishing a second receive channel through the second firewall, wherein the second response message is linked to the second HTTP message (FIG. 5B, step 512, page 7 lines 1-14, paragraph [34]);

(5) at the third computer, receiving a third encrypted HTTP message from the first computer through the first firewall; determining that the third encrypted HTTP message is intended to be delivered to the second computer, and transmitting to the second computer the third encrypted HTTP message, wherein the third encrypted HTTP message is transmitted over

the second receive channel through the second firewall to the second computer (FIG. 5C, steps 514, 516, page 3 lines 8-12, paragraph [08], page 7 lines 11-14, paragraph [34], page 8 lines 17-24, paragraph [40]; page 28 lines 12-27); and

(6) from the third computer, periodically transmitting "keep alive" messages to the first computer over the first receive channel and to the second computer over the second receive channel to avoid a time-out condition (page 13 lines 6-8, paragraph [61], page 23 lines 1-10).

Independent Claim 66

Independent method claim 66 recites a method of communicating between a first computer (FIG. 1, client 101) protected by a first firewall (FIG. 1, firewall 106, page 7 lines 1-14) and a second computer (FIG. 1, client 115) protected by a different second firewall (FIG. 1, 113) via a third intermediate computer (FIG. 1, server 107), comprising the steps of:

receiving at the third intermediate computer (FIG. 1, server 107, page 7 lines 1-14, FIG. 5A, step 506, page 7 lines 1-14, paragraph [34]) a request transmitted from the second computer through the second firewall, wherein the request is to establish a receive channel (page 22, lines 1-15) between the second computer and the third intermediate computer;

transmitting from the third intermediate computer a response to the request, the response establishing a receive channel between the third intermediate computer and the second computer that is to be kept open for subsequent transmissions by the third intermediate computer (FIG. 5A, step 507, page 22 lines 16-27);

receiving at the third intermediate computer data transmitted from the first computer through the first firewall via a network connection initiated by the first computer (FIG. 5C, step 514, page 3 lines 8-12, paragraph [08], page 8 lines 17-24, paragraph [40]);

determining that the data received from the first computer is intended to be delivered to the second computer (FIG. 5C, steps 514, 516, page 28 lines 9-16, paragraphs [139] and [140]); and

transmitting the data to the second computer via the receive channel (FIG. 5C, step 516, page 28 lines 27-28 to page 29 lines 1-6, paragraph [142]).

Independent Claim 74

Independent method claim 74 recites a method of communicating between a first computer (FIG. 1, client 101) protected by a first firewall (FIG. 1, firewall 106, page 7 lines 1-14) and a second computer (FIG. 1, client 115) protected by a different second firewall (FIG. 1 firewall 113) via a third intermediate computer (FIG. 1, server 107), from the perspective of the second computer (FIG. 1, client 115), comprising the steps of:

transmitting a request from the second computer (FIG. 1, client 115) to the third intermediate computer (FIG. 1, server 107) through the second firewall (FIG. 1, firewall 113) to establish a receive channel between the third intermediate computer and the second computer (page 7 lines 1-14, FIG. 5A, step 506, page 22, lines 19-22);

receiving from the third intermediate computer a response to the request, the response establishing a receive channel between the third intermediate computer and the second computer that is to be kept open for subsequent transmissions from the third intermediate computer (FIG. 5A, steps 507, page 22 lines 1-15); and

receiving data via the receive channel, wherein the data was transmitted from the first computer to the third intermediate computer through the first firewall via a network connection initiated by the first computer, then transmitted from the third intermediate computer to the second computer via the receive channel (FIG. 5C, step 514, page 3 lines 8-12, paragraph [08], page 8 lines 17-24, paragraph [40], page 28 lines 27-28 to page 29 lines 1-6, paragraph [142]).

Dependent Claim 56

No means plus function or step plus function limitations are contained in this claim. For the convenience of the examiner, dependent claim 56 recites the method of claim 55, further comprising the steps of, in the intermediate server computer (FIG. 1, server 107), decrypting encrypted information received from the first computer (FIG. 5C, server 502, substep 4) using encryption keys shared between the first computer and the intermediate computer (FIG. 5A, key exchange 508, page 24 lines 2-10), and then re-encrypting the received information (FIG. 5C, server 502, substep 5, page 16 lines 11-15) using encryption keys shared between the intermediate computer (FIG. 1, server 107, page 28 lines 5-16) and the second computer (FIG. 1, client 115).

Dependent Claim 59

No means plus function or step plus function limitations are contained in this claim. For the convenience of the examiner, dependent claim 56 recites the method of claim 55, wherein at least one of the HTTP POST messages (page 8 lines 15-24) transmitted during step (6) comprises an identifier of said second computer (FIG. 1, client 115, page 8 lines 10-24; page 26 lines 1-4; page 30 lines 14-21) encrypted with a first encryption key (FIG. 5C, step 514) associated with the intermediate server (FIG. 1, server 107), and wherein said encrypted information is encrypted with a second different encryption key (FIG. 5C, step 516) associated with the second computer (FIG. 1, client 115; page 31 lines 12-13; page 16 lines 7-14).

Dependent Claim 60

No means plus function or step plus function limitations are contained in this claim. For the convenience of the examiner, dependent claim 60 recites the method of claim 57, wherein the third encrypted HTTP message comprises an encrypted identifier of the second computer (FIG. 5C, client 501, 1. encrypt data, 2. encrypt first header), the identifier encrypted with a first encryption key associated with the third computer (id.), and encrypted content for delivery to the second computer, the content encrypted with a different second encryption key associated with the second computer (page 16 lines 7-15; page 31 lines 7-16; page 27 lines 25-26 to page 28 line 4).

Dependent Claim 63

No means plus function or step plus function limitations are contained in this claim. For the convenience of the examiner, dependent claim 60 recites the method of claim 55, wherein communication between the first computer (FIG. 1, client 101) and the intermediate server computer (FIG. 1, server 107) is initiated by the first computer (page 20 lines 10-12; page 21 lines 4-7), and wherein communication between the second computer (FIG. 1, client 115) and the intermediate server computer (FIG. 1, server 107) is initiated by the second computer (page 20 lines 10-12; page 7 lines 8-14; page 8 lines 19-22; page 14 lines 18-19).

Dependent Claim 70

No means plus function or step plus function limitations are contained in this claim. For the convenience of the examiner, dependent claim 70 recites the method of claim 66, wherein the data received from the first computer (FIG. 1, client 202) comprises an HTTP message encrypted using encryption keys shared between the first computer and the third intermediate computer (FIG. 1, server 107; FIG. 5C, step 514), and wherein the third intermediate computer (FIG. 1, server 107) decrypts the HTTP message received from the first computer and re-encrypts the HTTP message using encryption keys shared between the third intermediate computer and the second computer (FIG. 1, client 115; FIG. 5C, step 516; page 16 lines 11-15).

Dependent Claims 72 and 80

These claims are not argued separately but are instead grouped together for purposes of appeal. No means plus function or step plus function limitations are contained in these claims. For the convenience of the examiner, dependent claim 72 recites the method of claim 66, wherein communication between the first computer (FIG. 1, client 101) and the third intermediate computer (FIG. 1, server 107) is initiated by the first computer (page 20 lines 10-12; page 21 lines 4-7), and wherein communication between the second computer and the third intermediate computer is initiated by the second computer (page 20 lines 10-12; page 7 lines 8-14; page 8 lines 19-22; page 14 lines 18-19). Dependent claim 80 is identical but depends from independent claim 74 and is thus summarized in the same manner.

Dependent Claim 78

No means plus function or step plus function limitations are contained in this claim. For the convenience of the examiner, dependent claim 78 recites the method of claim 74, wherein the data received via the receive channel comprises an HTTP message (FIG. 5A, step 506, page 7 lines 1-14) from the first computer (FIG. 1, client 101), the HTTP message encrypted using encryption keys shared between the third intermediate computer (FIG. 1, server 107) and the second computer (FIG. 1, client 115, FIG. 5C, step 516, page 28 lines 5-16; page 31 lines 7-16).

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: February 12, 2008

By: /Bradley C. Wright/
Bradley C. Wright
Registration No. 38,061

1100 13th Street, N.W.
Suite 1200
Washington, D.C. 20005
Tel: (202) 824-3000
Fax: (202) 824-3001